Changing from Information Assurance to Cybersecurity?

<u>Information Assurance (IA)</u> - Measures that protect and defend <u>information</u> and <u>information systems</u> by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by

Department of Defense Directive (DoDD) 8500.01E, April 23, 2007

capabilities.

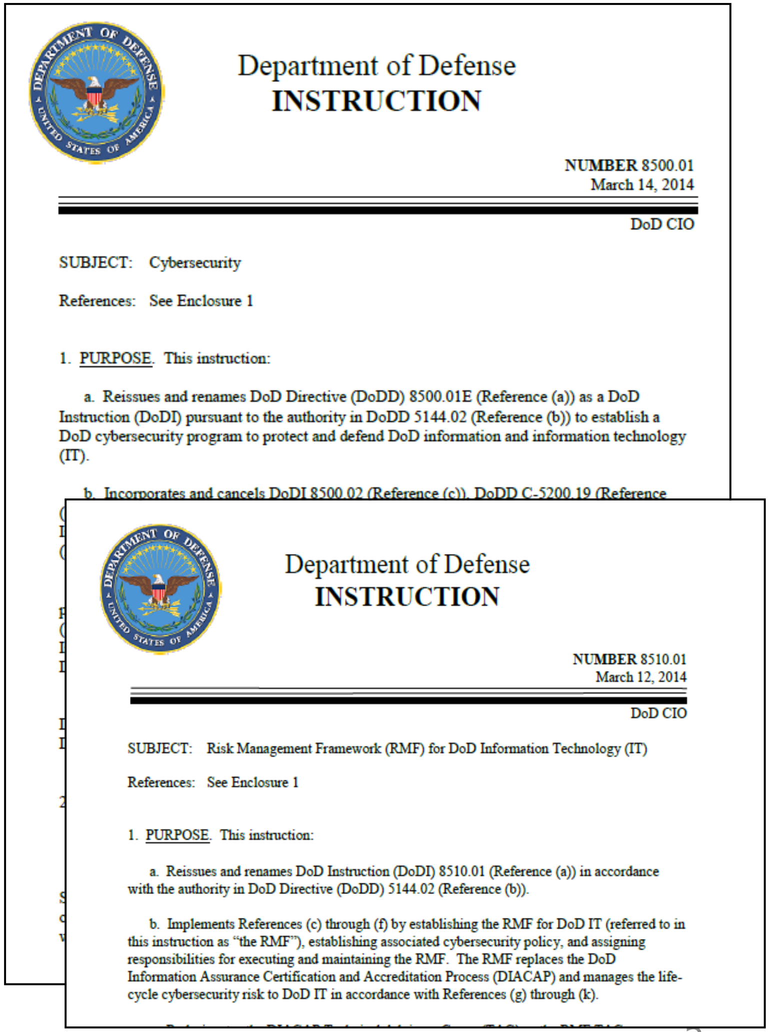
<u>Cybersecurity</u> - **<u>Prevention of</u>** damage to, protection of, and restoration of computers, electronic **<u>communications systems</u>**, electronic communications services, wire communication, and electronic communication, including <u>information contained therein</u>, to ensure its **availability,**

Department of Defense Instruction (DoDI) 8500.01, March 14, 2014

DoDI 8500.01 adopts the term "cybersecurity" to be used throughout the DoD instead of the term "information assurance (IA)."

DoD Risk Management Framework (RMF)

- DoD Instruction 8500.01
  - Cybersecurity
  - Signed March 14, 2014
- DoD Instruction 8510.01
  - Risk Management Framework (RMF) for DoD Information Technology (IT)
  - Signed March 12, 2014



Department of Defense
INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference

Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

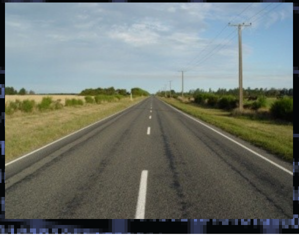
a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

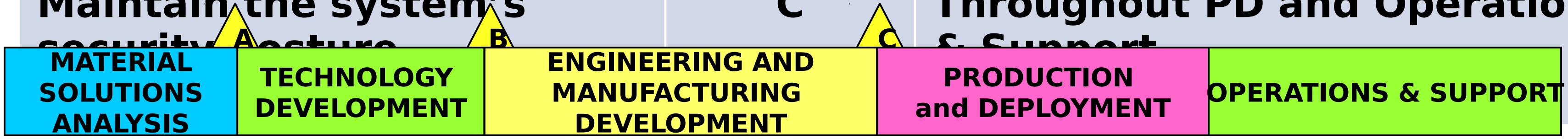
Cybersecurity RMF steps and activities, as described in DoD Instruction 8510.01, should be initiated as early as possible and fully integrated into the DoD acquisition process including requirements management, systems engineering, and test and evaluation.

DoDI 5000.02, January 7, 2015

IA Roadmap Under DIACAP



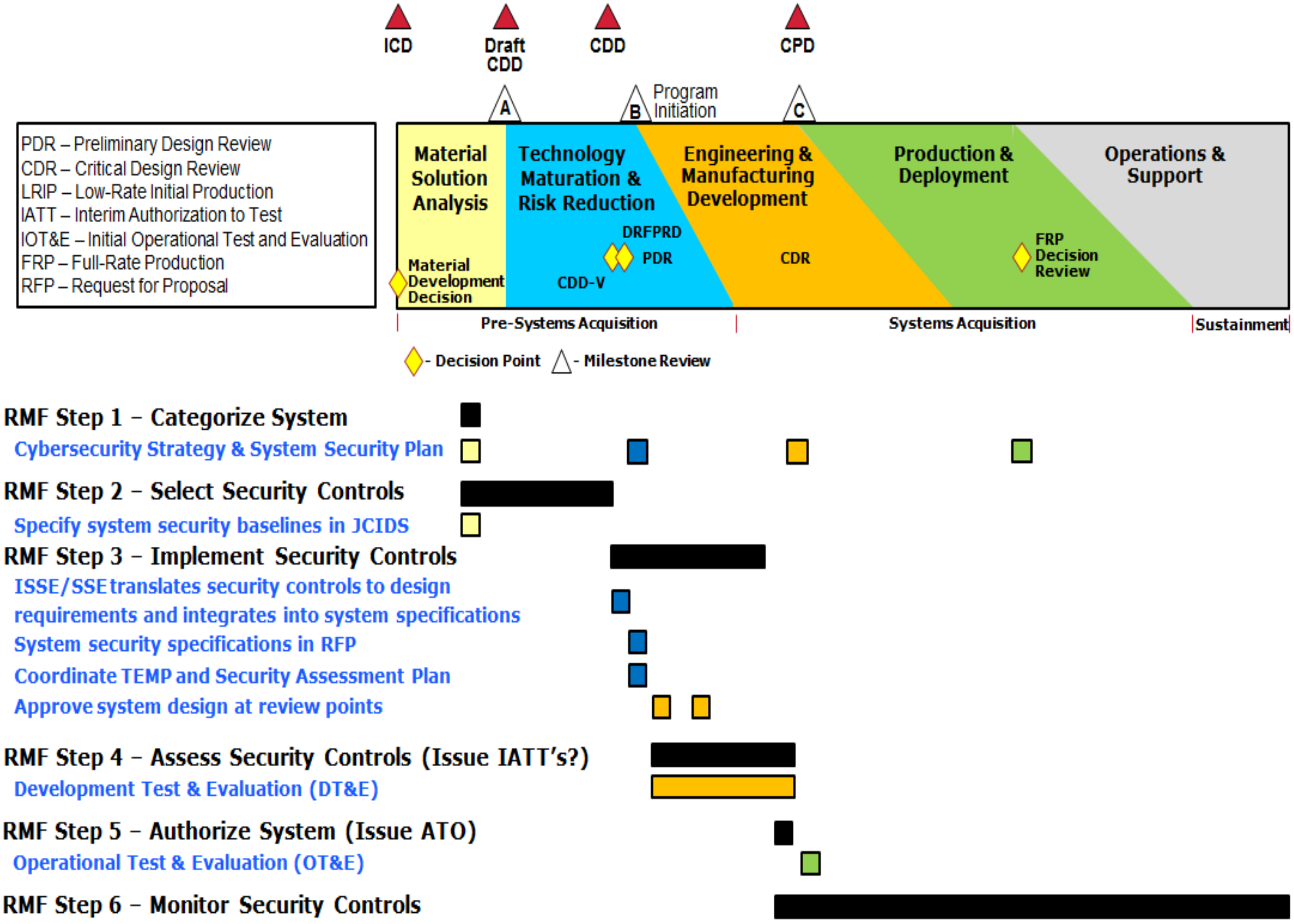
Roadmap step	Milestone	Phase of Lifecycle
Establish an IA organization	A	Early in Tech Development (TD)
Identify IA requirements	A	Early/mid stages of TD
Develop an acquisition IA strategy	A	Early/mid/late stages of TD
Secure resources for IA	A	Early/mid to late stages of TD
Initiate DIACAP	A	Mid TD to end of Engineering and Mfg Development (EMD)
Incorporate IA solutions	B	Mid/late TD to end of EMD
Test and evaluate IA solutions	B	Early/mid EMD to mid Production and Deployment (PD)
Accredit the system	C	Milestone C
Maintain the system's security posture	C	Throughout PD and Operations & Support



A
B
C
MATERIAL SOLUTIONS ANALYSIS
TECHNOLOGY DEVELOPMENT
ENGINEERING AND MANUFACTURING DEVELOPMENT
PRODUCTION and DEPLOYMENT
OPERATIONS & SUPPORT

RMF and the Acquisition Life Cycle

Cybersecurity requirements must be identified and included throughout the lifecycle of systems to include acquisition, design, development, developmental testing, operational testing, integration, implementation, operation,



PDR – Preliminary Design Review
CDR – Critical Design Review
LRIP – Low-Rate Initial Production
IATT – Interim Authorization to Test
IOT&E – Initial Operational Test and Evaluation
FRP – Full-Rate Production
RFP – Request for Proposal

ICD | Draft CDD | CDD | CPD

A | B Program Initiation | C

Material Solution Analysis | Technology Maturation & Risk Reduction | Engineering & Manufacturing Development | Production & Deployment | Operations & Support

Material Development Decision | DRFPRD | PDR | CDD-V | CDR | FRP Decision Review

Pre-Systems Acquisition | Systems Acquisition | Sustainment

◇ - Decision Point △ - Milestone Review

RMF Step 1 – Categorize System
Cybersecurity Strategy & System Security Plan

RMF Step 2 – Select Security Controls
Specify system security baselines in JCIDS

RMF Step 3 – Implement Security Controls
ISSE/SSE translates security controls to design requirements and integrates into system specifications
System security specifications in RFP
Coordinate TEMP and Security Assessment Plan
Approve system design at review points

RMF Step 4 – Assess Security Controls (Issue IATT's?)
Development Test & Evaluation (DT&E)

RMF Step 5 – Authorize System (Issue ATO)
Operational Test & Evaluation (OT&E)

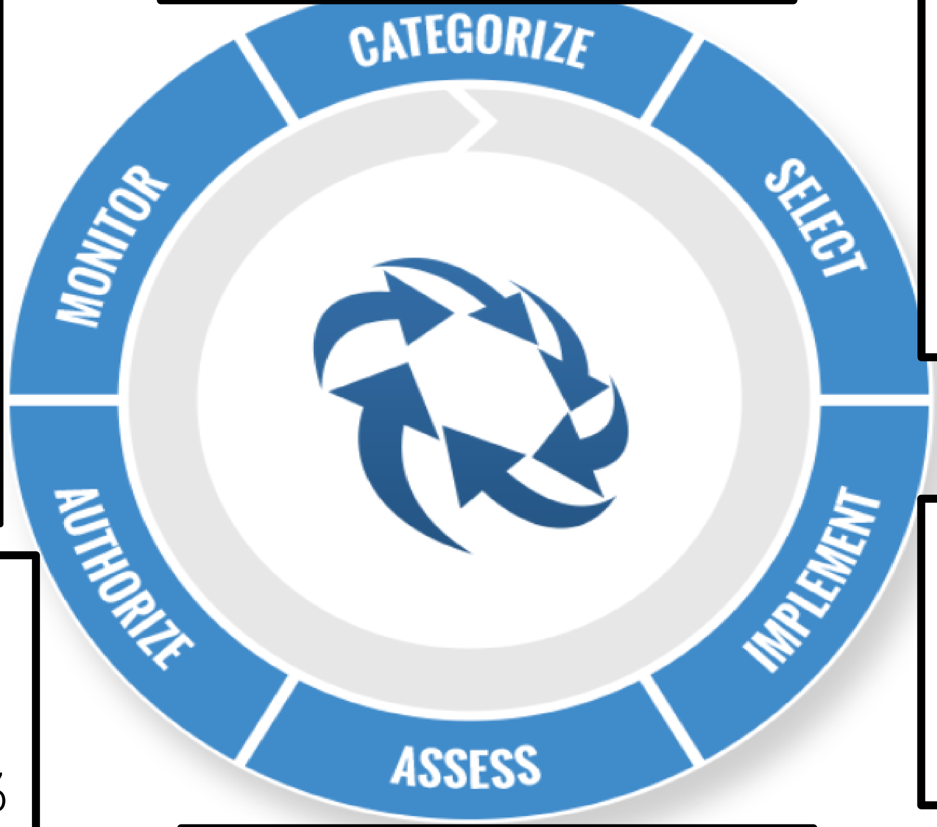
RMF Step 6 – Monitor Security Controls

RMF Process

Step 1: Categorize System
- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2: Select Security Controls
- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3: Implement Security Controls
- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan



Step 4: Assess Security Controls
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)

Step 5: Authorize System
- Prepare the POA&M
- Submit Security Authorization - - Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6: Monitor Security Controls
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR, and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF Transition Timeline (per RMF Knowledge Service)

Completed DIACAP Package Submitted to AO for Signature	ATO Date	Maximum Duration of ATO under DIACAP
Present through May 31, 2015	Determined by AO Signature Date	2.5 years from AO signature date
June 1, 2015 through February 1, 2016		2 years from AO signature date
February 2, 2016 through October 1, 2016		1.5 years from AO signature date

What this means:

The longer you stay with DIACAP, the shorter the ATO. DIACAP certified systems should be almost extinct by mid-year 2018.